NATIONAL INFRASTRUCTURE PROTECTION CENTER

HIGHLIGHTS

A publication providing information on infrastructure protection issues, with emphasis on computer and network security matters.

Issue 8-01
August 17, 2001

Editors: Linda Garrison
Martin Grand
Melissa Conaty

- **The Financial Services Information Sharing and Analysis Center**
- **Trends: Increasing Sophistication of Attacks Utilizing Malicious Code**
- **Security Concerns: Internet Based Applications**

For more information, or to be added to the distribution list, please contact the NIPC Watch at nipc.watch@fbi.gov or call (202) 323-3204.

We welcome your comments and suggestions for improving this product. To provide comments, contact the Editors at (202) 324-0334 or (202) 324-0353.

The Financial Services Information Sharing and Analysis Center

This article continues our series of overviews of critical infrastructure industry initiatives established in response to Presidential Decision Directive 63 (PDD-63).

The Financial Services Information Sharing and Analysis Center (FS/ISAC)

The FS/ISAC was the first ISAC to be established under PDD-63. Since 1999, the organization has grown in both size and in its capabilities to assist the banking and finance sector (collectively holding about $21 trillion of the U.S. financial sector's assets). Information about company membership in the ISAC is kept strictly confidential and shared only with those companies on the organization's Board of Directors. Bruce W. Moulton, Fidelity Investments, is the FS/ISAC's current chairperson. Stanley (Stash) R. Jarocki, Morgan Stanley and Dean Witter, serves as the FS/ISAC's treasurer.

The FS/ISAC provides the following services and products to its members to assist them in protecting their critical infrastructure:

- Anonymous information and incident submission and sharing
- Early notification of crisis and urgent alerts
- Multiple levels of incident analysis
- Trend data on threats, vulnerabilities, and incidents
- Security resolutions and recommendations

Status of FS/ISAC Activities

Recent meetings between the FS/ISAC and the NIPC have led to an enhanced relationship and a new information sharing agreement. In addition to the products available on the NIPC's public Web site [Warnings, CyberNotes, and Highlights (www.nipc.gov)], the NIPC has offered to share information that will be made available only to approved PDD-63 designated ISACs, such as the following:

- Special warnings and related information
- The NIPC's *Daily Report*
- Technical sanitized information concerning malicious code and exploits derived from unique analysis performed by the NIPC
- Information derived from the monthly Security Proof-of-Concept Keystone (SPOCK) forum

This unprecedented information sharing arrangement between the NIPC and the FS/ISAC will strengthen critical infrastructure protection efforts in the banking and finance sector. More information, including membership criteria, about the FS/ISAC is available on the organization's Web site at **http://www.fsisac.com**, or by contacting Stash Jarocki at 212-762-0211. Alternatively, the reader may contact Paul Rodgers at the NIPC by phone at 202-324-0341 or by e-mail at **prodgers@fbi.gov**.

Trends: Increasing Sophistication of Attacks Utilizing Malicious Code

The increasing sophistication of malicious software (malware) creates an opportunity for new types of attacks that take advantage of previously compromised hosts, which further necessitates the need for periodic updating of Anti-Virus software and vendor patches.

Observers of the computer security environment have noted a steady increase in the sophistication of attacks against individual computer systems over the past years.

New Trends

- *Increasingly crafty social engineering methods used by malware to dupe victims.*
  - The victim receives an e-mail, which appears to be a warning from a software vendor that promises to "detect, repair, and protect" against a well-known virus; in reality, the message contains a mechanism to infect the victim with a new virus.
  - E-mail messages used to propagate malware use eye-catching subject lines or a disarmingly routine text message in order to trick the recipient.

- *The appearance of new capabilities in malicious code.*
  - Some worms now contain their own Simple Mail Transfer Protocol (SMTP) engine, which the worm uses to send itself out independently of any e-mail software on the victim's computer.
  - Malware takes advantage of Internet hosts previously compromised by another malicious package such as a Trojan Horse program. The results of such attacks may result in the compromising of mass computer systems on the Internet as well as large-scale distributed denial-of-service (DDoS) attacks.

The speed with which worms can propagate across the Internet makes them ideal delivery mechanisms for setting up a network of clients that can be later exploited to launch DDoS or other types of attacks. In the near future, worms can be expected to evolve in multiple directions. They may become stealthier, contain more destructive payloads and become more lethal to computer systems.

With the rapidly evolving threat environment it is imperative that critical infrastructure operators adopt policies assuring that information security practices are implemented throughout their organization. For ways to protect ones system see www.cert.org under "What's New."

Security Concerns: Internet-Based Applications

Some software companies have a new vision for the way we communicate and do business every day, where the Internet not only acts as a conduit of information, but also as a dynamic "front end" to the tools we use. While this ease of use has many benefits, the potential for loss of data, loss of privacy and loss of availability might outweigh the benefits.

New Vision

Software companies envision an Internet that will replace the need to install applications directly onto a user's personal computer (PC). Common software applications such as word processing or spreadsheets would be accessible by subscription through an Internet browser. The need to purchase and install a program directly onto a user's PC would be eliminated because the user would subscribe only to the programs needed.

The benefits of this system are tremendous. Consumers would be able to receive the most current versions of software and have it delivered to them dynamically through the Internet. Because all upgrades are included in the time period covered by a subscription, the consumer would realize tremendous cost savings from not having to pay for each new version.

Potential Vulnerabilities

While this vision may be the next logical step in the evolution of the Internet, the potential dependence raises security concerns. For example, when a company is the victim of a Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack, its monetary losses are mainly from staff hours spent combating the attack and the potential sales or services lost due to being inaccessible during the attack. If the same company were dependent on some form of subscription service, the results of a loss could be devastating, in that during the attack not only are the people outside trying to access the company unable to do business, but the people inside are unable to do business as well.

It is not clear how the software companies developing these new services are planning on addressing the associated vulnerabilities. However, the DoS attacks mentioned above are some of the most basic attacks used by hackers today. Software companies will need to continue spending more time addressing the security issues associated with their innovative ideas.